Refine Search

Search Results -

Terms	Documents
6021202.pn.	2

Database:
US Pre-Grant Publication Full-Text Database
US Patents Full-Text Database
US OCR Full-Text Database
EPO Abstracts Database
JPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Search:

Refine Search

Recall Text

Clear

Interrupt

Search History

DATE: Saturday, February 18, 2006 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR			
L10	6021202.pn.	2	L10
L9	L8 and (account with holder or account near holder or account adj holder)	5	L9
L8	L7 and (establish$ or creat$) and authenticating near2 (record or document or file)	53	L8
L7	L6 and (financial near transactions or financial with transactions or financial adj transactions)	975	L7
L6	authentication and authorization and accounting	4658	L6
L5	L4 and 705/44	22	L5
L4	L2 and (establish$ or creat$) and authenticat$ near2 (record or document or file)	330	L4
L3	L2 and (establish$ or creat$) and authenticat$ near2 (record or document)	232	L3
L2	L1 and (financial near transactions or financial with transactions or financial adj transactions)	2312	L2

L1	authentication and authorization and account$	10326	L1

END OF SEARCH HISTORY

Hit List

First Hit | Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Search Results - Record(s) 1 through 5 of 5 returned.

☐ 1. Document ID: US 20050177521 A1

Using default format because multiple data bases are involved.

L9: Entry 1 of 5 File: PGPB Aug 11, 2005

PGPUB-DOCUMENT-NUMBER: 20050177521
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20050177521 A1

TITLE: Method for remotely authorizing a payment transaction file over an open network

PUBLICATION-DATE: August 11, 2005

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY
Crosson Smith, Steven A.	Winnersh Berkshire		GB

US-CL-CURRENT: 705/67

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw. De

☐ 2. Document ID: US 20050177504 A1

L9: Entry 2 of 5 File: PGPB Aug 11, 2005

PGPUB-DOCUMENT-NUMBER: 20050177504
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20050177504 A1

TITLE: System and method for remotely authorizing a payment transaction file over an open network

PUBLICATION-DATE: August 11, 2005

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY
Crosson Smith, Steven A.	Winnersh Berkshire		GB

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	COUNTRY	TYPE CODE
Bottomline Technologies (DE) Inc.	Portsmouth	NH		03

APPL-NO: 10/830830 [PALM]
DATE FILED: April 23, 2004

RELATED-US-APPL-DATA:
Application 10/830830 is a continuation-in-part-of US application 10/776407, filed February 10, 2004, PENDING

INT-CL-PUBLISHED: [07] G06 F 17/60

US-CL-PUBLISHED: 705/040; 705/064
US-CL-CURRENT: 705/40; 705/64

REPRESENTATIVE-FIGURES: 1

ABSTRACT:

A system is provided for approving an electronic fund transfer disbursement file and instructing a remote payment management system to generate and electronic fund transfer system to a payment processing server. The system comprises a network services module, a digital signature system and an electronic fund transfer submission module. The network services module establishes a secure connection to the remote payment management system. The digital signature system: i) returns a digital signature of a data file in response to a signature only processing call; and ii) returns a digital signature data structure in response to receiving a sign and package processing call. The electronic fund transfer submission module obtains an authorization request from the remote payment management system. The authorization request comprises a digest of the electronic fund transfer disbursement file. A dummy data file is passed to the digital signature system and a dummy data structure is returned. The dummy data structure comprises a dummy digest, a dummy digital signature of the dummy digest, and a digital certificate. The digest is also passed to the digital signature system and a digital signature of the digest is returned. An authentication data structure is build by replacing the dummy digest with the digest and replacing the dummy digital signature with the digital signature of the digest and is returned to the payment management system.

CROSS-REFERENCE TO RELATED ACTIONS

[0001] This application claims the benefit of, and is a continuation in part of U.S. patent application Ser. No. 10/776,407 filed on Feb. 10, 2004 entitled "Method for Remotely Authorizing a Payment Transaction File over an Open Network", the contents of such patent application being incorporated herein.

☐ 3. Document ID: US 20050177495 A1

L9: Entry 3 of 5 File: PGPB Aug 11, 2005

PGPUB-DOCUMENT-NUMBER: 20050177495
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20050177495 A1

TITLE: Payment processing system for remotely authorizing a payment transaction

file over an open network

PUBLICATION-DATE: August 11, 2005

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY
Crosson Smith, Steven A.	Winnersh Berkshire		GB

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	COUNTRY	TYPE CODE
Bottomline Technologies (DE) Inc.	Portsmouth	NH	US	02

APPL-NO: 10/776406 [PALM]
DATE FILED: February 10, 2004

INT-CL-PUBLISHED: [07] G06 F 17/60

US-CL-PUBLISHED: 705/039
US-CL-CURRENT: 705/39

REPRESENTATIVE-FIGURES: 1

ABSTRACT:

A payment management system for obtaining an approval of an electronic fund transfer (EFT) disbursement file from a user of a remote system and transferring the EFT disbursement file to a payments processor. The payment management system comprises an electronic fund transfer submission module for generating a digest, by performing a hash of the EFT disbursement file, and transferring the digest to the remote system along with authorization control code. The authorization control code drives the remote system to obtain a digital signature of authenticated attributes, which includes the digest, and generate an authorization response. The electronic fund transfer submission module further provides for receiving the authorization response from the remote system and transferring an electronic funds submission to the payments processor. The electronic funds submission comprises the payment transaction file and at least a portion of the authorization response comprising the digital signature.

☐ 4. Document ID: US 20050038756 A1

L9: Entry 4 of 5 File: PGPB Feb 17, 2005

PGPUB-DOCUMENT-NUMBER: 20050038756
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20050038756 A1

TITLE: System and method for production and authentication of original documents

PUBLICATION-DATE: February 17, 2005

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY
Nagel, Robert H.	New York	NY	US

APPL-NO: 10/894766 [PALM]
DATE FILED: July 20, 2004

RELATED-US-APPL-DATA:
Application 10/894766 is a division-of US application 09/577533, filed May 24, 2000, ABANDONED

INT-CL-PUBLISHED: [07] H04 L 9/00

US-CL-PUBLISHED: 705/076
US-CL-CURRENT: 705/76

REPRESENTATIVE-FIGURES: 1

ABSTRACT:

A system and method for authenticating documents and content thereof. A counterfeit resistant document recording medium is provided, having thereon a predefined unique document identifier and at least one security feature. The recording medium is thereafter imprinted with document content, which typically varies between documents. The document content is stored in a database, indexed by an associated document identifier. The document may then be authenticated by checking the security feature and comparing the stored document content with a perceived document content. The system provides a number of opportunities for commercial exploitation, including sales of identified recording media, recording of information in a database, on-line authentication transactions, differential accounting for document validations and counterfeit identifications, imprinting devices, authentication devices, and the like. The system prevents counterfeiting of valuable documents through casual means by providing both physical and logical security.

☐ 5. Document ID: US 6609200 B2

L9: Entry 5 of 5 File: USPT Aug 19, 2003

US-PAT-NO: 6609200
DOCUMENT-IDENTIFIER: US 6609200 B2

TITLE: Method and system for processing electronic documents

DATE-ISSUED: August 19, 2003

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Anderson; Milton	Fair Haven	NJ		

Jaffe; Frank	Boston	MA
Hibbert; Chris	Los Altos	CA
Virkki; Jyri	Scott Vly	CA
Kravitz; Jeffrey	Yorktown Heights	NY
Chang; Sheveling	Cupertino	CA
Palmer; Elaine	Goldens Bridge	NY

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY TYPE CODE
Financial Services Technology Consortium	New York	NY		02
International Business Machines Corporation	Hawthorne	NY		02
Sun Microsystems, Inc.	Palo Alto	CA		02
Clareon Corporation	Portland	ME		02
Telcordia Technologies, Inc.	Morristown	NJ		02

APPL-NO: 09/750379 [PALM]
DATE FILED: December 28, 2000

PARENT-CASE:
CLAIM OF PRIORITY This patent application is a continuation of U.S. patent application Ser. No. 09/386,551, now U.S. Pat. No. 6,209,095, entitled "Method and System for Processing Electronic Documents," filed on Aug. 31, 1999 and naming the same inventors as the present application, the contents of which are incorporated herein by reference, and which is a continuation of U.S. patent application Ser. No. 08/994,636, now U.S. Pat. No. 6,021,202, filed on Dec. 19, 1997 and naming the same inventors as the present application, the contents of which are incorporated herein by reference, and which further claims priority to U.S. patent application No. 60/033,896, entitled "Method and System for Processing Electronic Documents", filed on Dec. 20, 1996, the contents of which are incorporated herein by reference.

INT-CL-ISSUED: [07] H04 L 9/32, G06 F 17/27

US-CL-ISSUED: 713/176; 713/155, 713/160, 713/161, 713/181, 705/67
US-CL-CURRENT: 713/176; 705/67, 713/155, 713/160, 713/161, 713/181

FIELD-OF-CLASSIFICATION-SEARCH: 713/156, 713/160, 713/161, 713/164, 713/165, 713/170, 713/175, 713/176, 713/181, 705/67, 380/51, 380/54, 380/216
See application file for complete search history.

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
4302810	November 1981	Bouricius et al.	364/200
4423287	December 1983	Zeidler	178/22.08
4823264	April 1989	Deming	364/408
5005200	April 1991	Fischer	380/30
5187351	February 1993	Clary	235/379
5191613	March 1993	Graziano et al.	380/25

5214702	May 1993	Fischer	380/30
5218637	June 1993	Angebaud et al.	380/23
5224162	June 1993	Okamoto et al.	380/24
5283829	February 1994	Anderson	380/24
5297202	March 1994	Kapp et al.	380/9
5321751	June 1994	Ray et al.	380/23
5326959	July 1994	Perazza	235/379
5343530	August 1994	Viricel	380/23
5465299	November 1995	Matsumoto et al.	380/23
5473690	December 1995	Grimonprez et al.	380/24
5504818	April 1996	Okano	380/49
5521980	May 1996	Brands	380/30
5530755	June 1996	Pailles et al.	380/18
5532920	July 1996	Hartrick et al.	364/419.1
5557722	September 1996	DeRose et al.	395/148
5615268	March 1997	Bisbee et al.	380/25
5671282	September 1997	Wolff et al.	380/25
5673316	September 1997	Auerbach et al.	380/4
5673320	September 1997	Ray et al.	380/25
5677955	October 1997	Doggett et al.	380/24
5680461	October 1997	McManis	380/25
5708806	January 1998	DeRose et al.	395/615
5724523	March 1998	Longfield	395/235
5748738	May 1998	Bisbee et al.	380/25
5841970	November 1998	Tabuki	395/187.01
5864828	January 1999	Atkins	705/36
5905800	May 1999	Moskowitz et al.	380/28
5912974	June 1999	Holloway et al.	380/51
5943423	August 1999	Muftic	380/25
5956404	September 1999	Schneier et al.	380/25
6016484	January 2000	Williams et al.	705/39
6021202	February 2000	Anderson et al.	705/54
6209095	March 2001	Anderson et al.	713/176

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	CLASS
0 542 298	May 1993	EP	
0 542 298	May 1993	EP	
0 542 298	May 1993	EP	
WO 96/31965	October 1996	WO	

OTHER PUBLICATIONS

C. Kaufman et al., "Network Security: Private Communcation in a Public World," 1995, pp. 190-191.*
R.L. Rivest, A. Shamir, and L. Adelman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, vol. 21, No. 2, Feb.

1978, pps. 120-126.
"Electronic Authentication of Documents," New Mexico Statues Annotated 1978 .sctn..sctn. 14-15-1 to 14-15-6, including Proposed Rule effective Jul. 1, 1996.
"Applied Cryptography Second Edition: Protocols, Algorithms, and Source Code in C," Oct. 15, 1995, pps. 185-187.

ART-UNIT: 2132

PRIMARY-EXAMINER: Darrow; Justin T.

ATTY-AGENT-FIRM: Oliver; Kevin A. Foley, Hoag & Eliot LLP

ABSTRACT:

The invention includes a markup language according to the SGML standard in which document type definitions are created under which electronic documents are divided into blocks that are associated with logical fields that are specific to the type of block. Each of many different types of electronic documents can have a record mapping to a particular environment, such as a legacy environment of a banking network, a hospital's computer environment for electronic record keeping, a lending institution's computer environment for processing loan applications, or a court or arbitrator's computer system. Semantic document type definitions for various electronic document types (including, for example, electronic checks, mortgage applications, medical records, prescriptions, contracts, and the like) can be formed using mapping techniques between the logical content of the document and the block that is defined to include such content. Also, the various document types are preferably defined to satisfy existing customs, protocols and legal rules.

70 Claims, 44 Drawing figures

L9: Entry 5 of 5 File: USPT Aug 19, 2003

DOCUMENT-IDENTIFIER: US 6609200 B2
TITLE: Method and system for processing electronic documents

Abstract Text (1):
The invention includes a markup language according to the SGML standard in which document type definitions are created under which electronic documents are divided into blocks that are associated with logical fields that are specific to the type of block. Each of many different types of electronic documents can have a record mapping to a particular environment, such as a legacy environment of a banking network, a hospital's computer environment for electronic record keeping, a lending institution's computer environment for processing loan applications, or a court or arbitrator's computer system. Semantic document type definitions for various electronic document types (including, for example, electronic checks, mortgage applications, medical records, prescriptions, contracts, and the like) can be formed using mapping techniques between the logical content of the document and the block that is defined to include such content. Also, the various document types are preferably defined to satisfy existing customs, protocols and legal rules.

Brief Summary Text (11):
In addition to the problem of associating a signature with a document, other special problems are likely to exist in cases of documents that require signatures or affect commercial transactions. In particular, special requirements or protocols may apply to the content of such documents. For example, detailed rules exist as to how various actors are required to complete or respond to the information on each part of a paper check or other financial instrument. Similarly, rules exist as to how to complete and process a mortgage loan application. Different parts of medical records are also completed pursuant to protocols that require specific action on the part of medical personnel, insurers, and the like. In each of these cases the logical content of the different parts of the document is important, and a need exists to use the logical structure in the storage, manipulation and transmission of such document so that documents can be sent to known protocols. For example, if a protocol requires that a document bear a date, a logical element of the document should be defined for data information. Moreover, the protocols associated with signed documents are often established over time through custom and usage, so a need exists to permit electronic documents that closely mirror current practice. Also, although most individuals or businesses have computers, certain functions continue to be performed without the aid of a computer, such as viewing a human signature. Thus, it is important that documents that require signatures not only be machine processable, but also human readable.

Brief Summary Text (17):
With descriptive instead of procedural markup the same document can readily be processed by many different pieces of software, each of which can apply different processing instructions to those parts of it which are considered relevant. For example, a content analysis program might disregard entirely the footnotes embedded in an annotated text, while a formatting program might extract and collect them all together for printing at the end of each chapter. Different sorts of processing instructions can be associated with the same parts of the file. For example, one

program might extract names of persons and places from a document to create an index or database, while another, operating on text that has been "marked up" in some way, might print names of persons and places in a distinctive typeface.

Brief Summary Text (22):
SGML has the ability to use rules stating which elements can be nested within others to simplify markup. Such rules are the first stage in the creation of a formal specification for the structure of an SGML document, or document type definition. SGML is most useful in contexts where documents are seen as raw material to be matched against a pre-defined set of rules. Such rules can include legal rules or known protocols, customs or practices. By making the rules explicit, the designer reduces his or her own burdens in marking up and verifying the electronic text, while also being forced to make explicit an interpretation of the structure and significant particularities of the text being encoded.

Brief Summary Text (23):
A variety of software is available to assist in the tasks of creating, validating and processing SGML documents. At the heart of most such software is an SGML parser: that is, a piece of software which can take a document type definition and generate from it a software system capable of validating any document invoking that DTD. Output from a parser, at its simplest, is just "yes" (the document instance is valid) or "no" (it is not). Most parsers will however also produce a new version of the document instance in canonical form (typically with all end-tags supplied and entity references resolved) or formatted according to user specifications. This form can then be used by other pieces of software (loosely or tightly coupled with the parser) to provide additional functions, such as structured editing, formatting and database management.

Brief Summary Text (24):
A structured editor is a kind of intelligent word-processor. It can use information extracted from a processed DTD to prompt the user with information about which elements are required at different points in a document as the document is being created. It can also greatly simplify the task of preparing a document, for example by inserting tags automatically.

Brief Summary Text (27):
Hypertext systems improve on other methods of handling text by supporting associative links within and across documents. Again, the basic building block needed for such systems is also a basic building block of SGML markup: the ability to identify and to link together individual document elements is an inherent a part of the SGML protocol. By tagging links explicitly, rather than using proprietary software, developers of hypertexts can be sure that the resources they create will continue to be useful. To load an SGML document into a hypertext system requires only a processor which can correctly interpret SGML tags. HTTP servers in wide use for network computing are suitable to interpret SGML.

Brief Summary Text (28):
Although markup languages exist in accordance with the SGML standard that permit the user to manipulate documents according to logical content identified by tags within a document, conventional markup languages have not fully addressed the special problems associated with documents involved in signature transactions. A particular need exists for a flexible markup language that permits a document designer to create documents that are designed to comply with legal requirements and other protocols of a wide variety of particular transaction contexts that involve signatures. Also, a need exists for a markup language that permits the design of documents that are machine processable and human readable. A further need exists for electronic documents that can be subdivided or redacted as transmitted in parts, wherein the integrity of the document and the validity of the signature remains.

Brief Summary Text (30):
As seen in FIG. 1, in a typical financial transaction 10 a payer 12 transfers funds to a payee 14. Individual payers and payees prefer different payment methods at different times, including cash, checks, credit cards and debit cards. The transfer of funds between the payer 12 and the payee 14 may involve intermediate transactions with one or more banking institutions 16. The banks' functions include collecting and holding funds deposited by account holders and responding to instructions from the account holders. Checks are an example of financial transactions which invoke these banking institution functions.

Brief Summary Text (33):
After the payer 12 presents the completed check 22 to the payee 14 in a financial transaction (such as a sale of goods or services), the payee 14 endorses the check 22 on the back with instruction to deposit the amount 28 with the payee's bank 46. If the check looks authentic, the payee bank 46 provisionally credits the payee's account 48 for the amount of money designated on the face of the check 28 pending clearance through the federal reserve system and acceptance and payment by the payer's bank 36.

Brief Summary Text (34):
The payee's bank 46 routes the check 22 to the payer's bank, possibly using the federal reserve bank clearing house 50 or other established clearing arrangement, which uses the routing and transit number 25 to deliver it to the payer's bank 36, which then verifies the authenticity of the check 22 and (at least for some checks) the signature 38 of the payer 12. If the check 22 is authentic and the payer 12 has sufficient funds in her account 40 to cover the amount of the check 28, the payer's bank 36 debits the payer's account 40 and transfers funds to the payee's bank 46 for the amount designated on the check 28. A complete check transaction 20 thus includes verification steps performed by the payee 14 and the payer's and payee's banks 36 and 46.

Brief Summary Text (36):
Processing a paper check requires time as the physical check is routed to the payer, the payee, the payee's bank, the clearing house and/or the payer's bank. The same is true of other types of financial transactions involving paper instruments, such as credit card slips generated during a credit card sale. In a credit card transaction, a merchant makes an impression of the customer's card, which the customer then signs, to function as a receipt for the transaction. The merchant typically obtains a positive acknowledgment or credit authorization from the customer's credit card company before accepting the credit card slip. This assures that payment will be received.

Brief Summary Text (37):
Several mechanisms for using electronic communication to substitute for paper flow in financial transactions are in use or have been proposed.

Brief Summary Text (43):
Several systems are currently used to secure electronic financial transactions. For example, IC chip cards, or smart cards, are small devices (containing chips with memories) which are capable of exchanging data with a computer or a terminal and of performing simple data processing functions, and are thus more versatile than a simple credit card. The smart card is portable and may be easily used in POS and ATM environments.

Brief Summary Text (58):
The invention includes a computer-based method for creating a signed electronic documents.

Brief Summary Text (59):
In one aspect, the invention includes a markup language according to the SGML

standard in which document type definitions are created under which electronic documents are divided into blocks that are associated with logical fields that are specific to the type of block. Each of many different types of electronic documents can have a record mapping to a particular environment, such as a legacy environment of a banking network, a hospital's computer environment for electronic record keeping, a lending institution's computer environment for processing loan applications, or a court or arbitrator's computer system. Semantic document type definitions for various electronic document types (including, for example, electronic checks, mortgage applications, medical records, prescriptions, contracts, and the like) can be formed using mapping techniques between the logical content of the document and the block that is defined to include such content. Also, the various document types are preferably defined to satisfy existing customs, protocols and legal rules. For example, in the case where the electronic document is an electronic check, the document type definition for electronic checks can be designed to comply with Regulation E, of the Uniform Commercial Code and other state and federal laws for payment instruments. An example of a document type definition for the electronic check is depicted in FIG. 43. Where the document is a medical record, the document type definition can be designed to comply with health care regulations. When the document is a mortgage loan application, the document can be designed to comply with mortgage lending regulations. Other embodiments can be readily envisioned for other types of documents in other contexts that are legally required to have particular content. Document type definitions in FSML or SGML can thus be applied to legally significant communications, such as performative utterances, in a manner that permits the establishment of rules and protocols for handling content for that type of communication. Thus, a content block for the "pay to the order of" block of a check can be defined, and the associated computer software will treat the content in that block as the identification of the payee of the check. Similar protocols can be established for all types of significant content, including content relevant to business practices and legal rules.

Brief Summary Text (60):
In one embodiment, the invention features a computer-based method in which an electronic instrument is created for effecting a transfer of funds from an account of a payer in a funds-holding institution to a payee, the instrument including an electronic signature of the payer. A digital representation of a verifiable certificate by the institution of the authenticity of the account, the payer, and the public key of the payer is appended to the instrument. This enables a party receiving the instrument, e.g., the payee or a bank, to verify the payer's signature on the instrument. A similar certificate of authenticity could also be issued in other contexts. For example, a certifying authority could certify that a doctor is properly licensed and authorized to sign a prescription. A certifying authority could certify as to the creditworthiness of a borrower in a transaction. A certifying authority could certify as to the authority of an individual to sign a contract for a given company. These examples are merely illustrative of all transactions in which a certifying entity participates.

Brief Summary Text (65):
The signatures may be generated by public key cryptography. The appending step may be done by a separate signature device from the device which performs the creation of the electronic document.

Brief Summary Text (67):
Information may be automatically transferred from the electronic document to a computer-based data storage, manipulation, access and retrieval system, such as an accounting system that tracks accounts receivable or processes orders. A log or database of information about electronic document transactions may be created,

Brief Summary Text (70):
In general, in another aspect, the invention features a computer-based method of

creating an electronic document. Digital data is formed which represents the identity of each party to the transaction, and other relevant facts to the transaction, such as the amount to be paid in the case of an electronic check, or the amount of medicine in the case of an electronic prescription that is part of a medical record. Then, in a secure hardware token, a digital signature is appended to the data.

Brief Summary Text (72):
In general, in another aspect, the invention features a computer-based method for regulating the use of account numbers with respect to accounts in a funds-holding institution. Digital account numbers are assigned for use by account holders in creating electronic instruments, the digital account numbers being distinct from non-electronic account numbers used by account holders with respect to non-electronic instruments. At the funds-holding institution, electronic instruments are then accepted from account holders only if the electronic instruments include one of the digital account numbers. In implementations of this feature, each digital account number may be linked with a non-electronic account number, and the two numbers may be linked with a common account in the institution, so that electronic instruments and non-electronic instruments may be drawn against the same account. A similar aspect can be applied to regulating unique identifying numbers to information in a particular mortgage application, contract, medical record, or other electronic document.

Brief Summary Text (77):
The invention provides an all-electronic payments and deposit gathering instrument that can be initiated from a variety of devices, such as a personal computer, screen phone, ATM or payments accounting system. Financial accounts may be rapidly and securely settled between trading partners over open public or proprietary networks, without requiring pre-arrangement, by interconnection with the existing bank clearing and settlement systems infrastructure. The integration of controlled existing banking communication systems with rapidly growing public networks in a secure fashion will allow for implementation and acceptance by banking institutions, industry, and consumers.

Brief Summary Text (83):
The use of public-key certificates enables easy electronic authentication by a contracting party such as a payee of a check, and third parties such as the payee's and payer's banks. Digital signatures can be validated automatically.

Brief Summary Text (85):
In all embodiments, parties of all sizes gain substantial benefits. The use of electronic documents will be more cost effective than existing paper documents due to volume efficiencies and the automatic processing capabilities of computers. The use of electronic mail or electronic transmission is less costly than physically transporting paper. In addition to the significantly reduced costs of creating and mailing a document (no check stock, envelopes, stamps, photocopies or incremental labor), the party gains the ability to control the timing of transactions, such as payments, both through future dating of transactions and through the increased reliability and delivery speeds of electronic mail.

Brief Summary Text (87):
An electronic document may be signed and transmitted from personal financial software and other computing applications, through the use of an open programmatic tool set and application programming interfaces. Electronic instruments capability can be directly integrated into a payer's application, and does not require that a payer "go off-line" to complete a transaction. This benefit will be available to both consumers, through integrations with packages such as Intuit's Quicken.TM., and businesses through integration with existing accounting systems.

Brief Summary Text (91):

The term "client," as used herein, encompasses any data processing systems suitable for operating a processor according to the invention and for establishing a communication link to an Internet site. An Internet site can be any program running on a data processing platform that connects to the Internet and that receives access requests, whether under HTTP, FTP or any other conventional or proprietary transfer protocol.

Brief Summary Text (98):
The term "HTML" means hypertext markup language, which refers to languages for the creation of pages of the type capable of being viewed by a browser.

Drawing Description Text (2):
FIG. 1 is a block diagram of a financial transaction.

Detailed Description Text (5):
A Financial Services Markup Language (FSML) has been developed to allow for the creation of electronic documents that are human readable and machine readable and processable. FSML is a markup language according to the SGML standard. By using FSML, one can create, sign and process electronic documents. In an embodiment of the invention, the electronic documents may be electronic checks, and FSML may be used to create, sign and process electronic checks and their associated documents. In other embodiments, the documents may be medical records, loan applications, contracts, or the like. The creation of the electronic documents uses a block structure as noted below. The signing of the electronic documents can employ a public key cryptographic signature and hash algorithm to provide security attributes. The FSML signature mechanism also allows documents to be combined, or added to, without loss of the security attributes. The processing (e.g., signature verification, endorsements, authentication, payment, etc.) of the electronic documents is also automated.

Detailed Description Text (12):
The blocks include the relevant data for a transaction. Moreover, these document type definitions permit the establishment of rules that will reject a document that is missing some required element. For example, a contract may require an approval of a clause by a manager, and if approval is not included, the software of FSML would reject the document as an invalid type. Thus, document type definitions may be used to support legal rules and business practices.

Detailed Description Text (13):
The blocks making up the electronic document can be protected from tampering, and all blocks that need to be authenticated are assigned a digital signature contained in a signature block. The digital signature may use one of the standard digital signature algorithms, such as MD5/RSA or SHA/DSS. The digital signatures can be created using a private key, and then later verified using a public key which also can employ a certificate such as an X.509 Version 1 Certificate.

Detailed Description Text (19):
The digital signature is to insure that the electronic document is authentic and has not been tampered with. By using the multilevel hash operation, the electronic document is able to provide improved authentication and tamper resistance. The multilevel hash operation also allows various blocks or associated documents to be bound together while still providing improved authentication and tamper resistance. The digital signature can pertain to any of the blocks or a set of blocks. Further, improved authentication and tamper resistance allows blocks to be later dropped or remove from a bundle, yet the digital signature is still able to be authenticated. Thus, portions of documents may be transmitted and authenticated, while confidential portions are redacted.

Detailed Description Text (20):
Referring to FIG. 37, the calculation of a digital signature is performed as

follows. First, a nonce value (<nonce>) is created as a random number at step 600. The nonce value is used in producing a hash value as discussed below to enhance the security provided by the hash operation. Second, the nonce value is logically prepended to the subject block contents before hashing at a step 602. Third, at a step 604 a hash value is calculated using the contents of the subject block having the nonce value prepended, while excluding the block start tag and block end tag, but including all characters in between, with the exception of all carriage returns, line feeds, and trailing spaces on a line. Leading and embedded spaces in a line are included in the hash. SGML entities, i.e., character names enclosed between an ampersand (&) and a semicolon (;), are left untranslated when hashing. Fourth, at a step 608 the resulting hash value is inserted into the <hash> entry in the signature block. Fifth, at a step 610 the second through fourth steps are repeated for each block to be signed. Sixth, at a step 612 a second hash calculation is performed on the contents of the <sigdata> sub-block, which contains the previously calculated hashes, their block references, and the <nonce>. This includes all characters between <sigdata> tag and the </sigdata> tag, while admitting all carriage returns, line feeds and trailing spaces. Seventh, at a step 614 the second hash value is then encrypted using a private key. The result is the signature which is inserted (as Hex ASCII) into the signature block as the value for the <sig> tag.

Detailed Description Text (21):
An application programming interface (API) between an application program and an FSML electronic document is created by conventional programming means. The API allows developers of application programs to process electronic documents and associated documents without having to handle all of the details associated with the internal format and processing of these electronic documents. Instead, the API facilitates calls to an FSML Object Library that handles all the details of the internal format and processing of these electronic documents.

Detailed Description Text (22):
An FSML Object Library is described to handle processing that deals with the format and contents of FSML documents, an application program thus does not need to know about the actual format of an FSML document or any of the details of the interaction with a database application, such as an electronic checkbook. Likewise, the FSML Object Library will not need to know or care about details of hardware, operating systems, GUI's, databases, etc. In order to have platform independence, the FSML Object Library receives all input from the calling application program which also performs any necessary output. A call is made by the application program to create, parse, verify, modify, bind and otherwise operate on the memory-resonant FSML document. Functions are also provided to allow insertion and extraction of data items into and out of an FSML document.

Detailed Description Text (28):
The flexible document structures also permit the user to design documents that can be accessed by a wide range of transport systems and that can be manipulated by a wide range of computer systems. Thus, in the electronic check embodiment of the present invention, the instruments created with the present system may be accessed and manipulated by existing computer systems for demand deposit accounts.

Detailed Description Text (29):
Since it is created according to the SGML standard, a standard that is designed to permit easy interface to HTTP servers that are connected to the Internet, the present system is compatible with almost all computer network communications systems, including the Internet and local computer networks connected to the Internet by HTTP servers.

Detailed Description Text (30):
In an embodiment of the invention, an architecture for an electronic check system is disclosed. The electronic check system is an all-electronic payment and deposit

gathering instrument that can be initiated from a variety of devices, such as a personal computer, screen phone, ATM machine, or payments accounting system. The electronic check system provides rapid and secure settlement of financial accounts between trading partners over public or proprietary networks without requiring pre-arrangement.

Detailed Description Text (33):
As seen in FIG. 3, in a broad sense, a transaction is initiated when a payer 12, e.g., a consumer, electronically receives a memorandum of a proposed transaction 66, such as a bill, invoice or order form, from a payee 14, e.g. a merchant. Alternatively, a transaction may be initiated by the payer 12 only. The memorandum 66 may contain the payee's digital signature, which may be generated by the payee's secure authenticator 68 using public key cryptography. The payer 12 validates the payee's signature by using the payer's public key to verify the payee's digital signature and thus authenticates the payee 14. To proceed with the transaction, the payer 12 electronically creates a financial instrument 74, e.g., an electronic check (e.g., on a personal computer), payable to the order of the payee 14, and signs and records it using the payer's secure authenticator 70. In effect, the secure authenticator 70 enables the payer 12 to digitally sign the instrument 74 with a private signature key and enter the transaction in a secure log, such as an electronic check book 71. A record of the transaction may also be kept in the payee's accounting system 72. The authenticator also appends to the check cryptographically signed certificates of, e.g., the payer's bank and the federal reserve bank authenticating the payer's account and the payer's bank, respectively. The payer 12 then electronically sends the instrument 74 and the memorandum 66 via a public network 65 to the payee 14.

Detailed Description Text (36):
After clearance of the instrument, the payer's banking institution 82 receives the processed instrument 74. The payer's bank 82 validates both the payer's and the payee's signatures using public key cryptography. The payer's bank 82 also verifies that the instrument 74 is not a duplicate and that the date of the instrument 74 is valid, and checks the certificates. If there are sufficient funds to cover the face value of the instrument 74 in the payer's account, the payer's bank 82 debits the payer's account, treating the items as a normal DDA transaction, and electronically sends payment to the payee's bank 78 over the financial network 80 to settle the payment. The instrument 74 is archived for permanent storage and retrieval 83 at the payer's bank or elsewhere.

Detailed Description Text (37):
After the transaction has been completed, the payer's bank 82 issues a DDA statement 84 to the payer 12 reflecting the debit to the payer's account, and the payee's bank 78 issues a statement, report or accounts receivable update 86 to the payee 14 reflecting the credit to the payee's account. Supplementary information related to the transaction in the instrument 74, such as the payer's and payee's names or memo lines, can be included in the statement 84 or the report 86. The information contained in the statement 84 and the report 86 may be automatically compared with the payer's accounting system 72, and the payee's accounts receivable system 74, respectively, to verify that the transaction was carried out properly.

Detailed Description Text (38):
As seen in FIG. 4, an electronic document, such as an FSML document, such as an electronic check, may be created or verified and endorsed at a computer terminal or workstation, such as the payer's workstation 90 or the payee's workstation 92. Both workstations have the same general format. Each has a CPU with disk storage and memory and a keyboard, mouse and display for interaction with the user. Modems 91 and 93 (or other network connections) are attached to the workstations 90 and 92 and permit information, including the electronic check, to be passed electronically to other parties to the transaction via one of the electronic networks. Each workstation 90 and 92 also has a PCMCIA port 98 and 100, into which a signature

card, such as a PCMCIA card 94 or 96, may be inserted. The PCMCIA card 94 or 96 is an electronic device that acts as the user's digital signature card, provides a secure means for generating a signature with a private signature key, and acts as an electronic checkbook. Alternatively, the electronic checkbook with its register may be a separate card from the digital signature card.

Detailed Description Text (41):
The formatting of the electronic check has a number of embodiments. A preferred embodiment is as an FSML document, as described above. In another embodiment, the electronic check is formatted as a series of 7 bit ASCII text lines using a restricted character set in order to be compatible with a wide variety of electronic mail systems, including those implementing the Internet Simple Mail Transfer Protocol. The format of this other embodiment of the electronic check is based on tagged value pairs. Each information line is composed of a label name and a value, e.g., amount=$19.95. In this embodiment, an electronic check is typically created with a template document, as seen in FIG. 5. The top portion 106 of the template 105 contains the payee's remittance information. The bottom portion 107 of the template contains field that the payer completes to prepare the electronic check. The template may be sent by e-mail from the payee to the payer. In which case the payer can use an editor or word processor to enter order and remittance information. The check body can also be pre-formatted by the payee with the amount, "pay to the order of", and payer's public key lines already completed, allowing the payer to enter minimal information into the body of the electronic check before signing it. Alternatively, the payer can use a general template and an editor, word processor and other application, such as Quicken, to create a properly formatted electronic check.

Detailed Description Text (43):
For example, in FIG. 6, electronic check 110 contains an identification number for the electronic check 112, the date that the electronic check was created 114, an order to the bank to pay a certain sum of money 116, the name of the payee 118, the payee's public key, the sum of money to be paid 120, the payer's account number 122, the name, address and telephone number of the payer 124, and the payer's signature 126 in digital format verifiable using the payer's public signature key 134. An additional feature of an electronic check delivered over a public network is the payer's network address 128, e.g. an Internet address, to permit the payee to acknowledge receipt of the electronic check. The electronic check also may contain a memo block 130 for storing information personal to the payer and a secure hash algorithm (SHA) 132 resulting from a calculation over an associated document, to attach securely items such as an invoice received from the payee. The hash algorithm may be of the type more particularly described above.

Detailed Description Text (48):
The security and authentication aspects of electronic checks are supported by digital signatures using public key cryptography. Public key cryptography uses very large numbers and complex mathematical calculations to protect the integrity and secrecy of an encoded electronic transmission. As seen in FIG. 8, a digital cryptographic signature 101 is a long number or numbers (here expressed in hexadecimal notation) 102 which are produced by the signer's use of his private signature key and the message to be signed as inputs to the public key signature algorithm. The signature may also be accompanied by a date and time stamp 103. The cryptographic infrastructure is used to authenticate the payer and account, electronic check document and issuing bank, and to securely seal the electronic check, permitting the use of public networks for sending the electronic check. Most importantly, digital signatures may be used to verify a document after issuance.

Detailed Description Text (49):
A public key, applied to verify cryptographic digital signature, is always generated in conjunction with the private key which is used to create the signature. The payer's digital signature 126, the payer's public verification key

134, and the message which was signed are used as inputs to the public key signature verification algorithm, which produces a true or false value. Public key cryptographic signatures are useful because the signature of a signer, computed using the signer's private key, can be verified by anyone else who knows the signer's public key. Since the signer computes his signature on a document using his private key, and since the verifier verifies the signer's signature using the signer's public key, there must be a way for the verifier to trust the association between the signer (and his account information) and the public key used to verify the signer's signature on the electronic check. Cryptographic signatures are used to sign checks when they are written, co-signed, endorsed and processed. Cryptographic signatures are also used by certification authorities to sign certificates or "letters of reference" that contain a name or description of a signer and the signer's public key. Thus, anyone who trusts the certification authority and who knows the certification authority's widely publicized signature verification key can verify the certificate and trust the signer's public key for use in verifying the signer's signature.

Detailed Description Text (52):
Tamper-resistant signature cards or other hardware devices are useful to compute the cryptographic digital signatures without the possibility of disclosing the signer's private signature key. Tamper-proofing of an electronic check and associated information is achieved using digital signatures and a secure hash algorithm. Signature cards, or special cryptographic processors, can be used to better secure the private keys and greatly reduce the need for diligence and skill on the part of the account holders to secure their keys, especially against attacks through network connections by computer hackers. Further, the signature card may keep a non-erasable log of documents signed, so that the holder can review whether all uses of the card have been legitimate.

Detailed Description Text (53):
The digital signature is to insure that the electronic document is authentic and has not been tampered with. By using the multilevel hash operation, the electronic document is able to provide improved authentication and tamper resistance. The multilevel hash operation also allows various blocks or associated documents to be bound together while still providing improved authentication and tamper resistance. The digital signature can pertain to any of the blocks or a set of blocks. Further, improved authentication and tamper resistance allows blocks to be later dropped or remove from a bundle yet the digital signature is still able to be authenticated.

Detailed Description Text (54):
Referring still to FIG. 6, one difference between an electronic check and a paper check is the presence of authenticating certificates, in particular an account certificate 136 and a bank certificate 138. The payer can expedite the establishment of trust among the parties to the transaction by enclosing with the signed check a "letter of reference" or cryptographic certificate 136 regarding the payer's account, stating the payer's name, address and telephone number 124 and Internet address 128, account number 122, and public signature verification key 134, signed by the bank holding the payer's account with its digital signature private key 140. Similarly, a second letter of reference or certificate 38 regarding the payer' bank states the payer's bank's name 142, address 144, electronic network routing code 146 and public signature verification key 134, signed by the bank holding the payer's account with its digital signature private key 140. Similarly, a second letter of reference or certificate 38 regarding the payer's bank states the payer's bank's name 142, address 144, electronic network routing code 146 and public signature verification key 148, signed by a central body such as the federal reserve with its digital signature private key 150. Therefore, anyone knowing the federal reserve's public signature verification key 152 can sequentially verify the bank's certificate 138, the account certificate 136, and then the payer's signature 126 on the electronic check.

Detailed Description Text (60):
Upon endorsing the electronic check, the payee creates a deposit instrument 160 which is attached to the electronic check 110, as shown in FIG. 6. The deposit instrument 160 may be an FSML document type and may contain some of the same information as in the endorsement, such as the payee's account number. The deposit instrument 160 contains an identification number 162, the date 164, and the sum of money to be deposited 166. It also contains the payee's account number 168, the name, address and telephone number of the payee 170, the payee's Internet address 174 and the payee's signature 175 in digital format readable using the payee's public signature key 172. The deposit instrument 160 also may contain a memo line 180,

Detailed Description Text (68):
A PCMCIA card is an electronic device that provides greater security for a financial transaction. A PCMCIA card, or in the case of mainframe accounting systems, a secure black box, e.g. a Racal's Guardata, protects transactional systems from unauthorized access. The PCMCIA card is a separate, narrowly defined, secure electronic environment used in conjunction with a terminal such as a personal computer. Information passes back and forth between the PCMCIA card and the terminal or workstation.

Detailed Description Text (72):
The electronic check book contains a register 222 that functions like a conventional checkbook register, but without account balances. When an electronic check is created, the electronic check number, date, amount, payee, signature and hash are recorded in a check log 224. For each deposit made into the electronic check account endorsed by the electronic checkbook, the deposit number, date and amount are stored in an endorsement log 226. If the electronic checkbook has the capability, there may also be entries for bank fees and interest earned on the account. Integrating the electronic checkbook with other software applications would allow the electronic check account to be automatically balanced. Since the register may only have a limited memory space, the oldest transactional items are removed automatically when the memory has been exhausted.

Detailed Description Text (77):
The only function which must be performed by the PCMCIA card is creating the signature, since the payer's private signature key can never be allowed to leave the PCMCIA card, for security reasons. However, better security is achieved if the SHA of the electronic check is also performed by the PCMCIA card, so that the PCMCIA can be sure that the number, date, payee and amount logged into the PCMCIA card are the ones used in the computation of the SHA.

Detailed Description Text (78):
The electronic checkbook is issued by the bank that holds the electronic checking account. Initialized electronic checkbooks may be sent to the account holder, in which case the PIN should be sent separately for security reasons. Alternatively, uninitialized cards may be distributed to bank branches. The bank officer can then use a trusted initialization terminal and a special smart card identifying the bank officer to establish a secure connection to a centralized CIS. The new card is inserted into the terminal to be initialized. This method has the advantage of making electronic checkbooks immediately available to new customers, accounts can be added to electronic checkbooks already being used by the customer, and certificates can be refreshed prior to their expiration dates without issuing new electronic checkbooks. The bank, or its agent, is also acting as a certifying authority since it is responsible for authenticating the identity of the electronic checkbook and PIN are delivered to the correct person. The electronic check may also support correspondent banking relationships, and will allow another bank or approved third party to act as a stand-in processor for electronic checks for banks that are unable to directly support the processing requirements for electronic checks. This will facilitate electronic check deployment in a secure way without

affecting the traditional bank-customer relationship.

Detailed Description Text (79):
Similar functions to those of the PCMCIA card can be served by large scale cryptographic processors, such as Atalla or Racal Guardata boxes, for large operations where individual signature cards are impractical. For servers or mainframes which issue or endorse a large volume of checks, or which issue or endorse checks on behalf of a number of account holders, the processing and key storage capacities of signature cards may be exceeded. In this case, special cryptographic hardware must be used.

Detailed Description Text (83):
For example, as seen in FIG. 11, a certified electronic check involves a payer 12 creating an electronic check in the usual manner as described above. Certified checks are endorsed and cashed similar to normal checks, except that the payee 14 is guaranteed that the funds are available. The payer 12 e-mails the electronic check to the payer's bank 36 for certification. The bank may require the use of privacy enhanced mail or an equivalent to ensure the identity of the enhanced mail or an equivalent to ensure the identity of the payer and that the communication with the payer is confidential. The bank will then append a certifying signature to the check and e-mail it back to the payer. Upon receipt of the certified electronic check, the payee can verify the bank's certification signature as part of the validation of the check.

Detailed Description Text (86):
The formats of an electronic check and the entire electronic check system will be uniform, so that the electronic check system may be interconnected and used in conjunction with standard Application Programming Interfaces (API's), such as standard electronic checkbook interfaces and electronic check display interfaces. API's apply on the level of individual check processing as well as integration of the entire system. For example, the C language may be used to define an electronic check with field such as the date, the amount and the payee. Also, the Internet World Wide Web browser interacts with the electronic checkbook using an API to create the complete electronic check. The electronic check API's do not change, so that the system may be interfaced with any system by rewriting the particular system API and the link to the electronic check system.

Detailed Description Text (90):
There is a base set of supporting modules. These base modules provide for the creation, destruction, and manipulation of a parameterized electronic financial instrument (the electronic check), the interpretation of such instruments as electronic checks, the generation and verification of digital signatures on the payment instruments, and the interaction with electronic checkbook hardware devices.

Detailed Description Text (91):
API functions for supporting the application needs described include a "write" function, for creating an electronic check, binding it to an attached document (if present) and signing the electronic check; a "co-sign" function, for appending a second signature to the electronic check; a "verify" function, for verifying signatures on a check and validating the binding to an associated document (if present); an "endorse" function, for verifying signatures on the check and if valid, appending an endorsement and signing the check to be deposited or cashed; a "register read" function, for reading the contents of the check register contained in the electronic checkbook; and a "registry entry" function, for appending an entry to the check register.

Detailed Description Text (92):
For example, an electronic check an be attached to electronic remittance information provided by a remote payee. This enables the payment to be made, routed

correctly and automatically posted to both parties' accounting systems. Integration with micropayment accounting systems for high volume, small value financial transactions will enable those systems to settle accounts using an electronic check. The standardization of the electronic checkbook interfaces and the API's to access electronic checkbook functions simplifies integration with a variety of home and small business accounting and communications software packages. By defining the layout of the electronic check, the information it contains (e.g., account number and amount) can be readily extracted from the electronic check and used in other applications through the API's.

Detailed Description Text (99):
The security measures discussed above will eliminate most of the causes of losses due to bad checks, including forgery, alteration, duplication, and fraudulent depositing. Forgery is prevented by ensuring that digital signature keys are stored in secure hardware devices and through appropriate controls over the validity of electronic check certificates. Alteration is prevented by the application of digital signatures to the electronic check and through the use of the SHA function which creates a unique digest of the electronic document.

Detailed Description Text (104):
Tamper-resistance of the PCMCIA card is also needed to the extent necessary to make it economically unattractive for attackers to steal signature cards, extract the private key, and pass bad checks using the private signature key before the card is reported stolen and disabled. Any attempt to extract the private signature key should result in evident alteration of the card and should take at least a few days to succeed. However, an extremely high degree of tamper-proofing is not necessary, since the card only contains private information for one or several accounts (rather than system level secrets) and since the card holder has an incentive to report theft or tampering (rather than to extract a secret to use for fraud or counterfeiting).

Detailed Description Text (108):
The flexible document structures also permit the user to design documents that can be accessed by a wide range of transport systems and that can be manipulated by a wide range of computer systems. Thus, in the electronic check embodiment of the present invention, the instruments created with the present system may be accessed and manipulated by existing computer systems for demand deposit accounts.

Detailed Description Text (112):
As seen in FIG. 25, a mortgage transaction may also take advantage of a network 561. The borrower 452 may sign the loan application 490 with the borrower's secure authenticator 554 which permits a digital signature of the loan application 490. A database 556 of the borrower's system permits the borrower to record the transaction. Once the borrower has signed the loan application 490, it may be transmitted by the network 561 to the lender 454. The lender may digitally sign the loan application 490 using the lender's secure authenticator 558. This transaction may be recorded by the lender's database 560. Once the broker 455 has signed the loan application 490, it may be transmitted via the network 561 through a network connection 462 to a proprietary network or intranet 564 of one or more banking institutions 456. Signatures, authentication, data manipulations, storage and retrieval, and other functions are accomplished in a manner similar to that used for the electronic check.

Detailed Description Text (113):
Referring to FIG. 28, the hardware necessary for participation of the borrower and lender in a mortgage loan transaction is depicted in which a borrower workstation 630 is provided including various components similar to the components required for the electronic check or financial transaction. The lender workstation 632 is similarly configured. Software for preparation and manipulation of loan applications are also located on the workstations 630 and 632.

Detailed Description Text (114):
Referring to FIG. 26, the transmission of a medical record 520 is depicted wherein a first doctor 462 signs the medical record or a portion thereof 520 with the first doctor's secure authenticator 566 which permits a digital signature of the medical record 520. The signature may then be recorded in a database 570 which is responsive to the first doctor's secure authenticator. Once signed, the medical record 520 may be transmitted to a third party or to a second doctor 464. The second doctor may add material including a signature using the second doctor's secure authenticator 568. The second doctor's database 572 will record the signature and the additional information. Once signed by one or more doctors, the medical record 520 may be sent by a network 574 through a network connection 576 to a proprietary system 578 of one or more third parties 468, which could include an insurance company an administrative, or the like. Signatures, authentication, data manipulations, storage and retrieval, and other functions are accomplished in a manner similar to that used for the electronic check.

Detailed Description Text (115):
Referring to FIG. 29, the hardware required for a medical record transaction or transmission is provided in which a first doctor workstation 660 and a second doctor workstation 662 are provided. The workstations are similarly configured to the workstations necessary for other transactions of the present invention, such as an electronic check transaction, or the execution of a contract. Software residing on the workstations 660 and 662 may include applications for creating and manipulating medical records, including wage processing software.

Other Reference Publication (3):
"Electronic Authentication of Documents," New Mexico Statues Annotated 1978 .sctn..sctn. 14-15-1 to 14-15-6, including Proposed Rule effective Jul. 1, 1996.

CLAIMS:

1. A markup language for authenticating a document, the markup language in the form of program code embodied on a computer-readable medium, the markup language comprising instructions to determine a document type by the constituent parts of the document and the structure of the document, the document being human readable and machine readable, separate the document into blocks, assign a digital signature to one or more of the blocks, and, insert at least one of a start-tag at a beginning of the blocks and an end-tag at an end of the blocks.

18. A system for authenticating a document, comprising: a first programmable digital computer, the first programmable digital computer including, a definition module to determine a document type by the constituent parts of the document and the structure oft document, the document being human readable and machine readable; a block module to separate the document into blocks, the block module comprising a tag module to insert at least one of a start-tag at a beginning of the blocks and an end-tag at an end of the blocks; and a signature module to assign a digital signature to one or more of the blocks.

45. A markup language for authenticating a document the markup language in the form of program code embodied on a computer-readable medium, the markup language comprises instructions to parse a document into fields, the document being human readable and machine readable, associate the fields with blocks and at least one of a start-tag at a beginning of the blocks and an end-tap at an end of the blocks, and assign a digital signature of at least one of the blocks.

58. A system for authenticating a document, the system comprising: a first programmable digital computer, the first programmable digital computer including, a parse module to parse the document into fields, the document being human readable

and machine readable, an association module to associate the fields with blocks and at least one of a start-tag at a beginning of the blocks and an end-tag at an end of the blocks, and a signature module to assign a digital signature to at least one of the blocks.

Previous Doc Next Doc Go to Doc#